IN THE CLAIMS:

Claims 1 - 12 (Cancelled)

13. (Original) A method for use in a multi-level secure system for sanitizing a message, said multi-level secure system including at least first and second security levels wherein first security level users are authorized to receive sensitive information that second security level users are not authorized to receive, said method comprising the steps of:

establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules;

first using said computer-based sanitization tool for receiving a message for potential distribution;

second operating said computer-based sanitization tool for identifying at least first and second potential recipients having first and second security clearances, respectively;

third operating said computer-based sanitization tool for sanitizing said received message to generate a first sanitized message for transmission to said first potential recipient; and

fourth operating said computer-based sanitization tool for sanitizing said received message to generate a second sanitized message, different than the first sanitized message, for transmission to said second potential recipient.

14. (Original) A method as set forth in Claim 13, wherein said step of third operating comprises identifying first sensitive information within said message based on said first security clearance of said first potential recipient and protecting said first sensitive information such that said first sensitive information is not useable by said first potential recipient, and said step of fourth operating comprises identifying second sensitive information based on said second security clearance of said second potential recipient and protecting said second sensitive information such that said second sensitive information is not useable by said second potential recipient.

15. (Original) A method as set forth in Claim 13, wherein said step of third operating comprises accessing storage including multiple rule sets, using a parameter associated with said first security clearance to select a first rule set, and applying said selected first rule set with

respect to said message to generate said first sanitized message, and said step of fourth operating comprises accessing said storage including said multiple rule sets, using a second parameter associated with said second security clearance to select a second rule set, and applying said second rule set with respect to said message to generate said second sanitized message.

16. (Original) A method as set forth in Claim 13, wherein said step of first using comprises receiving a text only message.

17. (Original) A method as set forth in Claim 13, wherein said message includes a graphics portion and said step of third operating comprises protecting sensitive information within said graphics portion such that said sensitive information is not useable by said first recipient.

18. (Original) A method as set forth in Claim 13, wherein said step of third operating comprises parsing said message into a number of tokens and separately analyzing each token for sensitive information.

19. (Original) A method as set forth in Claim 13, wherein said step of third operating comprises identifying a first format associated with said first potential recipient and converting said first sanitized message into said first format, and said step of fourth operating comprises identifying a second format associated with said second potential recipient and converting said second sanitized message into said second format.

20. (Original) A method as set forth in Claim 19, further comprising the step of providing storage including first specification information for said first format and second specification information for said second format, where said step of third operating comprises accessing said storage to obtain said first specification information and said step of fourth operating comprises accessing said storage to obtain said second specification information, wherein said storage can be used to reconfigure said sanitization tool for transmission in multiple formats without re-compiling.

Claims 21 – 29 (Cancelled)

30. (Previously Presented) A method for use in a multi-level secure system for sanitizing a message, said method comprising steps of:

receiving an input file that includes information associated with at least first and second security levels of the multi-level secure system, wherein a user associated with said first security level of the multi-level secure system is entitled to receive information that a user associated with said second security level of the multi-level secure system is not entitled to receive;

determining a security level associated with at least one user of the multi-level secure system to be said second security level;

parsing intelligible elements from the information of the input file;

analyzing said intelligible elements to select a portion of the intelligible elements for sanitization according to the second security level;

sanitizing the information of the selected portion of the intelligible elements according to the second security level to generate an output file for said at least one user of the multi-level secure system, wherein said output file has a first format; and

formatting the output file to a second format for said at least one user of the multi-level secure system; and

transferring the output file in the second format to said at least one user of the multi-level secure system.

31. (New) A method for use in a multi-level secure system for sanitizing a message, said method comprising the steps of:

establishing rules based logic for use in determining a level of access to sensitive information as a function of information regarding an intended recipient of a message including at least a portion of said sensitive information, wherein different recipients are associated with different levels of access to said sensitive information, said rules based logic further being operative for analyzing specific items of said sensitive information in the context of a given message relative to a selected rule set of a number of rule sets, wherein different ones of said rule sets correspond to set different levels of access to said sensitive information;

receiving, in a processing system including said rules based logic, a first message including a first item of said sensitive information;

analyzing, in said processing system, said first message to obtain recipient information regarding a first intended recipient of said first message;

based on said recipient information, accessing a first rule of a first rule set of said number of rule sets using said processing system;

applying said first rule to process said first item of sensitive information, using said processing system, so as to generate a processed first message having a difference in relation to said first message, said difference being a function of said recipient information regarding said first intended recipient; and

operating said processing system to cause said processed first message to be transmitted to said first intended recipient.

32. (New) A method as set forth in Claim 31, further including processing the said first item of sensitive information according to the first rule, wherein said processing includes altering the first item of sensitive information or removing the first item of sensitive information.

33. (New) A method as set forth in Claim 32, further including processing the first message according to a second rule associated with a second recipient to generate a second message that differs from the first message.

34. (New) A method as set forth in Claim 33, wherein processing the first message includes processing a second item of sensitive information according to the second rule, wherein said processing the second item of sensitive information includes altering the second item of sensitive information or removing the second item of sensitive information.